UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,064	08/22/2003	Paul Moroney	D03037	9712

43471 7590 08/07/2009

Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
08/07/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	10/647,064	MORONEY ET AL.	
	Examiner	Art Unit	
	ELLEN TRAN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2009 and 03 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication filed on: Petition decision mailed on 21 July 2009 in response to petition and amendment filed 3 June 2009. The original application filed was filed on 22 August 2003, with acknowledgement of priority date of 23 August 2002, based on provisional application filing of 60/405,537.

2. Claims 1-29 are currently pending in this application. Claims 1, 11, and 18 are independent claims. Claims 1 and 5-23 have been amended. Amendments to the claims are accepted.

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed 3 June 2009 has been entered.

Response to Arguments

4. Applicant's arguments filed 3 June 2009 have been fully considered however they are moot due to new grounds of rejection initiated by applicant's amendment to the independent claims or not persuasive where noted below.

I) In response to applicant's argument beginning on page 9, *"Neither Candelore '489 nor Candelore '162, taken along or in combination disclose or suggest the claimed invention ... Candelore '489 does not disclose to use a key register in a first body which cannot be overwritten after a programmability period"*.

This argument is moot because the Craft reference teaches 'a key register in a first body which cannot be overwritten after a programmability period' as shown below in paragraph 42. Note the 'programmability period' is interpreted equivalent to the 'manufacturing process which ends when the CPU chip is released to the customer.

II) In response to applicant's argument beginning on page 10, *"the hard drive locking key discussed in Candelore '162 is not used for encryption to produce ciphertext, and hence is not analogous art to Applicant's invention as it is not in the same field of endeavor or concerned with the same problems faced by Applicant"*

The Examiner disagrees, as previously indicated Candelore '162 and Candelore '489 share a common inventor and are both assigned to Sony. In addition Candelore '162 is specifically directed to hard drive and it is explained in Candelore '162 that hard drives are incorporating in many customer appliances such as 'set-top' boxes in paragraphs 3 and 5. Candelore '162 in paragraphs 9 and 27 as well as Fig. 1a, teaches that one embodiment is 'the hard drive coupled to a set-top box'. It is well known in the art that set-top boxes are used by cable providers to distribute electronic digital content which is encrypted or scrambled. Therefore Candelore '162 is directed to the same field of endeavor and there is a motivation to combine.

Claim Objections

5. Claims 5-23 are objected to because of the following informalities: The status of the claims is incorrect in addition the amendments to the claims are not reflected accurately. For example claim 5 is not the original presented claim as submitted on 22 August 2003 it is actually the original of claim 6. Claim 6 which applicant indicates as 'Original' is not the originally

presented claim 6. In addition claim 11 appears to be claim 13 amended as well as claim 18 is actually and amended version of claim 23. The claims 5-23 each contain multiple errors indicating the correct status, it appears that applicant was looking at different set of claims rather than the original set submitted on 22 August 2003. It appears that claims 6, 8, 12, 14, 19, 20, 22, and 23 are new or newly presented amended limitations. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 6 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 and 12 indicate "decrypting the first key the key encryption key, whereby the first key is protected with the key encryption key outside the first package". In the claim it is unclear, 'indefinite' what is the 'key encryption key' is it the first key, second key, or third key. As best understood the limitation is protecting all the keys from being decrypted outside of the first chip package.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art

to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 1-23 and 25-29,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore U.S. Patent 6,697,489 (hereinafter '489) in view of Craft et al. US Patent Application Publication 20020150243 (hereinafter '243).

As to independent claim 11, "A method for protecting interchip content pathways transporting digital content objects within a content processing unit, the method comprising steps of: loading a first key into a first key storage register in a first chip package, wherein the first key in the first key storage register is non-readable from outside the first chip package" is taught in '489 col. 6, lines 16-58, note the first chip package is interpreted equivalent to the conditional access unit that includes a smartcard interface, a CPU, and a descrambler integrated circuit, the first key that is non-readable from outside is interpreted equivalent to the key used to decrypt the control word is stored in hardware in register 450 in IC440;

"encrypting digital content with the first key to produce ciphertext content" is disclosed in col. 6, lines 37-48, note the encrypting digital content is interpreted equivalent to the 'control word transferred in encrypted form that can only be decrypted by the 'first key', i.e. key stored in register 450;

"coupling the ciphertext content from the first chip package to a content pathway; loading a second key into a second key storage register in a second chip package" is shown in '489 col. 7, lines 20-36, the decryption engine uses the CW, i.e. the second key to produce

plaintext content, the second chip package is interpreted equivalent to the smartcard which loads CWs or second keys;

"wherein the second key in the second key storage register is non-readable from outside the second chip package, the second key storage register being writeable while being non-readable; coupling the ciphertext content from the content pathway to a second chip package; and decrypting the ciphertext content with the second key to reformulate the digital content" is disclosed in '489 col. 7, lines 59 through col. 8, the keys (i.e. second or third or next key) is loaded into the Descrambler IC as needed. Since the keys are stored in encrypted form they are not accessible outside of the Descrambler IC, furthermore it is known in the art that content within a smartcard is not readable outside the smartcard;

the following is not explicitly taught in '489: **"activating a feature of the first chip package that prevents overwriting the first key in the first key storage register from outside the first chip package, after a period in which the first key is loaded in the first key storage"**

however '243 teaches in paragraph 0042 "Each client CPU chip has a cryptographic unit that has been manufactured to contain programmable memory storage. Prior to releasing a client CPU chip, the manufacturer permanently embeds or fixes the assigned client serial number, the assigned client private key, and the server public key into the CPU chip. As shown in FIG. 2, client CPU chip 212 contains cryptographic unit 214, which includes client serial number 216, client private key 218, and server public key 220. A variety of well-known methods are available for embedding binary data within semiconductor chips, such as blowing semiconductor fuses as is used in DRAM manufacturing".

It would have been obvious to one of ordinary skill in the art at the time of the invention a method copy management system taught in '489 to include a means to program permanent keys into storage. One of ordinary skill in the art would have been motivated to perform such a modification to maintain control of distributed copyrighted content see '243 (page 2, paragraphs 13-14).

As to dependent claim 12, **"further comprising steps of: loading a key encryption key into a third key storage register in the first chip package; and decrypting the first key with the key encryption key, whereby the first key is protected with the key encryption key outside the first chip package"** is taught in '489 col. 7, line 59 thru col. 8, line 3, "In an alternative embodiment as shown in FIG. 7, the smart card may b replaced by the headend710 of a one-or two-way network … The Keys are decrypted only in the Descrabler IC 740, by using the Descrambler IC Unique Keys stored in register 750", therefore all key are prevented from being decrypted outside the chip package, the headend710 is interpreted equivalent to the 'third key storage.

As to dependent claim 13, **"further comprising a step of overwriting the second key in the second key storage register from outside the second chip package"** is taught in '489 col. 7, lines 15-20 that the unique key can be changed with a EMM message in '489.

As to dependent claim 14, **"further comprising steps of: encrypting the digital content in the second chip package to produce second ciphertext content using the second or another key that is a function of the second key, coupling the second ciphertext content to a second content pathway** is shown in '489 col. 7, line 59 through col. 8, line 28.

As to dependent claim 15, **"wherein: the content processing unit is part of a larger system comprising a plurality of functionally equivalent content processing units, and each of the plurality uses a different first key to protect their respective content pathways"** is disclosed in '489 teaches that the unique keys can be programmed during manufacture of the set top, TV, or NRSS-B module and '489 teaches that the traditional smart card could be replaced with a headend in col. 7, lines 59-65, the headend can deliver service keys encrypted based on the unique of the IC descrambler, the larger system is the cable network.

As to dependent claims 16 and 17, these claims are directed to a computer system or computer readable medium adapted to perform the computer-implementable method of claim 11 therefore they are rejected along similar rationale.

As to independent claim 1, "A content processing unit for protecting interchip content pathways transporting digital content objects, the content processing unit comprising: a first chip package, wherein the first chip package comprises a first body" is taught in '489 col. 6, lines 16-58, note the first chip package is interpreted equivalent to the conditional access unit that includes a smartcard interface, a CPU, and a descrambler integrated circuit, the first key that is non-readable from outside is interpreted equivalent to the key used to decrypt the control word is stored in hardware in register 450 in IC440;

"a first plurality of interconnects" '489 teaches a plurality of interconnects to the conditional access units such as by smart card and channels used to receive messages over the cable network in col. 5, lines 29-54;

"an encryption engine, and" is shown in '489 col. 6, lines 3-5, note the descrambler integrated circuit 440 in interpreted to be an encryption enginet;

"a first key storage register capable of storing a first key wherein: the first key is used by the encryption engine to produce ciphertext content, the first key storage register is non-readable from outside the first body" is taught in '489 col. 6, lines 16-58, note the first chip package is interpreted equivalent to the conditional access unit that includes a smartcard interface, a CPU, and a descrambler integrated circuit, the first key that is non-readable from outside is interpreted equivalent to the key used to decrypt the control word is stored in hardware in register 450 in IC440, note the encrypting digital content is interpreted equivalent to the 'control word transferred in encrypted form that can only be decrypted by the 'first key', i.e. key stored in register 450;

"a second chip package, wherein the second chip package comprises: a second body, a second plurality of interconnects, a decryption engine", is taught in '489 col. 5, lines 29-49 using an external or second encryption engine such as a smart card and that 'there are different types of security architectures for conditional access units', i.e. plurality of interconnects;

"and a second key storage register capable of storing a second key, wherein: the second key is used by the decryption engine to produce plaintext content from the ciphertext content" is shown in '489 col. 7, lines 30-36, the decryption engine uses the CW, i.e. the second key to produce plaintext content;

"and the second key storage register is non-readable from outside the second body, the second key storage register being writeable while being non-readable" is disclosed in '489 col. 6, lines 26-36;

"a content pathway coupling a first subset of the first plurality and a second subset of the second plurality, wherein the content pathway transports the digital content objects as the ciphertext content" '489 teaches utilizing the smart card to receive encrypted CW and saving this CW for later use in col. 7, line 59 through col. 8, line 7;

the following is not explicitly taught in '489: **"and the first key storage register cannot be overwritten after a programmability period, the programmability period being a period in which the first key is loaded in the first key storage"** however '243 teaches in paragraph 0042 "Each client CPU chip has a cryptographic unit that has been manufactured to contain programmable memory storage. Prior to releasing a client CPU chip, the manufacturer permanently embeds or fixes the assigned client serial number, the assigned client private key, and the server public key into the CPU chip. As shown in FIG. 2, client CPU chip 212 contains cryptographic unit 214, which includes client serial number 216, client private key 218, and server public key 220. A variety of well-known methods are available for embedding binary data within semiconductor chips, such as blowing semiconductor fuses as is used in DRAM manufacturing".

It would have been obvious to one of ordinary skill in the art at the time of the invention a method copy management system taught in '489 to include a means to program permanent keys into storage. One of ordinary skill in the art would have been motivated to perform such a

modification to maintain control of distributed copyrighted content see '243 (page 2, paragraphs 13-14).

As to dependent claim 2, "wherein the programmability period ends when a command is sent to the first plurality" is taught in '489 col. 7, lines 15-20 that the unique key can be changed with an EMM message in '489.

As to dependent claim 3, "wherein the command activates a fusable link" however '243 teaches in paragraph 42 'that binary data can be embedded within semiconductor chips, such as blowing semiconductor fuses as is used in DRAM manufacturing'.

As to dependent claim 4, **"wherein the programmability period ends after writing to the first key storage register"** however '243 teaches in paragraph 42.

As to dependent claim 5, **"wherein at least one of the first and second chip packages comprises a plurality of semiconductor substrates"** is taught in '489 col. 7, lines 1-15.

As to dependent claim 6, this claim is substantially similar to claim 12; therefore it is rejected along similar rationale

As to dependent claim 7, "wherein the second key storage register is overwritable by manipulating the second plurality" '489 teaches that the CWs could only be valid for a certain period of time and that the register can store multiple keys, therefore it is obvious that the second key storage register would be over written.

As to dependent claim 8, "wherein the second chip package further comprises a second encryption engine, and the second encryption engine uses the second key or another

key that is a function of the second key" '489 teaches that the key management can be performed both internal and externally by using an external or second encryption engine such as a smart card in col. 5, lines 29-49.

As to dependent claim 9, "further comprising a third chip package comprising a third key that can decrypt ciphertext produced with the second encryption engine" is disclosed in '489 col. 7, line 59 through col. 8, line 19, note the smartcard can be replaced by a headend, 'i.e. third chip package';

"wherein: the second chip package further comprises a second encryption engine, and the second encryption engine uses the second key or another key that is a function of the second key to encrypt the content object or a derivative thereof" is shown in '489 col. 7, line 59 through col. 8, line 19.

As to dependent claim 10, "wherein: the content processing unit is part of a larger system comprising a third plurality of functionally equivalent content processing units, and each of the third plurality uses a different first key to protect their respective content pathways" is disclosed in '489 teaches that the unique keys can be programmed during manufacture of the set top, TV, or NRSS-B module and '489 teaches that the traditional smart card could be replaced with a headend in col. 7, lines 59-65, the headend can deliver service keys encrypted based on the unique of the IC descrambler, the larger system is the cable network.

As to independent claim 23, this claim contains substantially similar subject matter as independent claim 1; therefore it is rejected along the same rationale.

As to dependent claim 25, "wherein: at least one of the first and second chip packages further comprises a key encryption key, and at least one of the first and second

keys is protected with the key encryption key outside the first body" is taught in '489 col. 5, lines 29-32 and col. 6, lines 16-36.

As to dependent claim 26-29, these claims contain substantially similar subject matter as claims 8-11; therefore they are rejected along similar rationale.

It is noted that any citations to specific, pages, columns, lines, or figures in the prior art references and any interpretation of the references should not be considered to be limiting in any way. A reference is relevant for all it contains and may be relied upon for all that it would have reasonably suggested to one having ordinary skill in the art. See, MPEP 2123.

10. **Claim 24,** is rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore U.S. Patent 6,697,489 (hereinafter '489) in view of Craft et al. US Patent Application Publication 20020150243 (hereinafter '243) in further view of Candelore et al. US Patent Application Publication No. 2003/0188162 (hereinafter '162).

As to dependent claim 24, the following is not explicitly taught in the combination of '489 and '243: **"wherein: the first key storage register has a third plurality of bits, and each of the third plurality can only change its stored value, at most, one time"** however '162 teaches "In one embodiment, the lock bit is written to one time programmable (OTP) memory and not changeable. In alternative embodiments, the lock bit may be re-programmable. Under the right conditions, the use of a master key may be used to revert the hard drive to an un-locked condition" on page 3, paragraph 0040.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method copy management system taught in '489 and '243 to include a means to utilize OTP methods to change keys. One of ordinary skill in the art would have been motivated to perform

such a modification improve upon the use of hard drives with host systems such as set-top boxes to facilitate repair see '243 paragraphs 5, 25, and 40.

Conclusion

11. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123).

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2433
30 July 2009